Ein Sieg für die Sicherheit – aber welche? Der Beschluss des BVerfG zur Nutzung von IT-Sicherheitslücken beim Einsatz von Staatstrojanern

JuWiss Redaktion

2021-08-05T14:00:55

von
THERESA BOSL

Seit einigen Tagen ist die Ausspähsoftware „Pegasus“ in aller Munde – eine Software, die nicht nur alle Daten eines Mobiltelefons durch das Ausnutzen von Sicherheitslücken auslesen, sondern auch verschlüsselte Kommunikation mitlesen und Kamera und Mikrofon nutzen kann. Diese Software wurde eigentlich Behörden für die Kriminalitätsbekämpfung zur Verfügung gestellt. Neuere Erkenntnisse zeigen jedoch, dass diese Software auch genutzt wurde, um politische Gegner*innen oder Systemkritiker*innen sowie Politiker*innen anderer Staaten auszuspionieren. Just im Zuge dieser Aufdeckungen veröffentlichte das Bundesverfassungsgericht am 21.07.2021 einen Beschluss (BvR 2771/18), in dem es die staatliche Nutzung vergleichbarer Software für verfassungsgemäß erklärte.

Der Einsatz von Staatstrojanern und die Ausnutzung von Sicherheitslücken

Heutzutage steht die digitale Kommunikation längst im Fokus der Sicherheitsbehörden, insbesondere im Bereich der Terrorismusbekämpfung. Damit der digitale Raum von Terrorist*innen nicht ausgenutzt werden kann, um staatlichen Maßnahmen zu entgehen, setzen Sicherheitsbehörden sogenannte Staatstrojaner ein. Damit kann auch verschlüsselte Kommunikation in die Ermittlungen einbezogen werden. Bei dem Einsatz des „kleinen“ Staatstrojaners, der Quellen-Telekommunikationsüberwachung (Quellen-TKÜ), wird eine laufende digitale Kommunikation überwacht. Bei dem Einsatz des „großen“ Staatstrojaners, der

Online-Durchsuchung, hingegen wird ein gesamtes informationstechnisches System und dessen Datenbestand ausgewertet. Die Staatstrojaner können auf verschiedene Weisen eingesetzt werden. So ist es denkbar, dass Ermittelnde physischen Zugriff auf das Gerät einer Zielperson nehmen, um hierauf eine entsprechende Software zu installieren. Möglich ist aber auch ein Zugriff aus der Ferne, für den bestehende Sicherheitslücken – etwa in Betriebssystemen oder einzelnen Anwendungen – verwendet werden, um auf rein digitalem Wege die Überwachung zu ermöglichen. Dabei kann man wiederum zwischen Fällen unterscheiden, in denen der System- oder Softwarehersteller bereits seit einem gewissen Zeitraum Kenntnis von der Sicherheitslücke hat (sog. N-Day-Schwachstellen) und Fällen, in denen der Hersteller keine solche Kenntnis besitzt (sog. Zero-Day-Schwachstellen). Auch die „Pegasus“-Software nutzt genau solche Schwachstellen aus.

Verfassungsbeschwerde gegen die Risiken von Zero-Day-Schwachstellen

In dem der Entscheidung des Bundesverfassungsgerichts zugrunde liegenden Sachverhalt ging es um den Einsatz von Staatstrojanern unter Nutzung dieser Zero-Day-Schwachstellen, wenn auch nicht in einem mit „Pegasus“ vergleichbaren Umfang. Die Beschwerdeführenden wandten sich mit ihrer Verfassungsbeschwerde gegen § 54 Abs. 2 des Polizeigesetzes Baden-Württemberg (PolG BW). Dieser erlaubt den Einsatz einer Quellen-TKÜ, also die Überwachung laufender Kommunikation, zur Abwehr terroristischer Gefahren. Die Verfassungsbeschwerde griff den Umstand an, dass § 54 PolG BW eine solche Online-Durchsuchung auch durch die Nutzung von Zero-Day-Schwachstellen erlaube. Diese Tatsache führe zu erheblichen Sicherheitsrisiken, da auch Dritte diese Schwachstellen ausnutzen könnten. Somit seien nicht nur die Daten der Personen im Visier der Sicherheitsbehörden, sondern aller Bürger*innen, die das betroffene informationstechnische System nutzten, betroffen. Dritte könnten, so die Befürchtung, diese Lücken nicht nur zur Überwachung laufender Kommunikation, sondern auch zur Auswertung des gesamten Datenbestandes des informationstechnischen Systems missbrauchen. Die Beschwerdeführenden sahen ihr Grundrecht auf die Vertraulichkeit und Integrität informationstechnischer Systeme („IT-Grundrecht“) dadurch verletzt, dass die Sicherheitsbehörden bei Zero-Day-Schwachstellen keine Meldepflicht an den Hersteller treffe. Hilfsweise richteten sie ihre Verfassungsbeschwerde darauf, dass für die Nutzung von Zero-Day-Schwachstellen keine gesetzlich vorgeschriebenen Kriterien zum Umgang mit den genutzten Sicherheitslücken vorlägen.

Staatliche Schutzpflichten aus dem IT-Grundrecht

Im Fokus des Beschlusses des Bundesverfassungsgerichts steht somit nicht die Abwehr-, sondern die aus der objektiven Dimension folgende Schutzpflichtenfunktion der Grundrechte, konkret des IT-Grundrechts. Dabei betont die Entscheidung, dass Zero-Day-Schwachstellen eine besonders schutzbedürftige Position der Bürger*innen berühren, die zum einen auf dem besonderen Persönlichkeitsbezug des IT-Grundrechts beruht, zum anderen auf der Tatsache, dass informationstechnische Systeme breit genutzt werden und

daher eine hohe Wahrscheinlichkeit für eine Betroffenheit der informationellen Selbstbestimmung besteht. Erlangt der Staat Kenntnis über solche Schwachstellen, über die die Bürger*innen selbst keinen Einblick erlangen können, verdichtet sich der allgemeine Auftrag des Staates, die Daten seiner Bürger*innen zu schützen, zu einer konkreten Schutzpflicht (Rn. 34). Ob diese im konkreten Fall verletzt wurde, prüfte das Bundesverfassungsgericht allerdings nicht. Stattdessen wies es die Verfassungsbeschwerde bereits als unzulässig zurück, da die Ausführungen der Beschwerdeführenden der im Falle von Schutzpflichten erhöhten Darlegungslast nicht genügt hätten (Rn. 53 ff.).

Dennoch sind die Ausführungen des Gerichts beachtenswert: In dem Beschluss erörterten die Verfassungsrichter, dass die Nutzung von Zero-Day-Schwachstellen das Aufstellen von gesetzlichen Regeln zur Auflösung des „Zielkonflikts“ bei dem Einsatz von Staatstrojanern verlangt (Rn. 34). Dieser Konflikt berührt zwei Aspekte der grundrechtlichen Schutzpflichtendimension: Zum einen ist der Staat dazu verpflichtet, die innere Sicherheit zu gewährleisten und seine Bürger*innen nach Möglichkeit vor terroristischen Akten zu schützen. Die heimliche Infiltration von informationstechnischen Systemen ist dazu ein geeignetes Mittel (vgl. BVerfG, 1 BvR 370/07, Rn. 221). Auf der anderen Seite ist der Staat dazu verpflichtet, seine Bürger*innen davor zu schützen, dass Dritte diese Lücken ebenfalls nutzen und damit ihr Recht auf informationelle Selbstbestimmung beeinträchtigen (Rn. 34). Das Bundesverfassungsgericht verlangt daher, dass der Gesetzgeber der Exekutive eine Abwägung der gegenläufigen Belange für den Fall aufgeben muss, dass ihr eine Zero-Day-Schutzlücke bekannt wird. Hierfür muss der Gesetzgeber selbst konkrete Vorgaben aufstellen. Diese wiederum müssen die Gefahr einer weiteren Verbreitung der Kenntnis von Sicherheitslücken einerseits und den qualitativen und quantitativen Nutzen möglicher behördlicher Infiltrationen mittels dieser Lücken andererseits umfassen (Rn. 44).

Ein Sieg für die Sicherheit – aber welche?

Mit dem Beschluss hat das Bundesverfassungsgericht die Ausnutzung von Zero-Day-Schwachstellen grundsätzlich als verfassungsgemäß anerkannt. Zur Nutzung sind aber konkrete Kriterien und eine umfassende Evaluation durch entsprechend ausgebildete Expert*innen vonnöten, um die Daten unbescholtener Bürger*innen effektiv zu schützen. Es stellt sich aber die Frage, wie effektiv dieser Schutz tatsächlich sein kann, wenn bekannte Schwachstellen nicht behoben werden. Die jüngsten Aufdeckungen zu der Pegasus-Software haben gezeigt, wie real und wie weit verbreitet das Missbrauchsrisiko ist – und dass entsprechende Schadsoftware, wenn sie einmal in der Welt ist, leicht der Kontrolle des Staates entgleiten kann. Die Entscheidung über die Nutzung von Sicherheitslücken verlangt eine offene Debatte in Wissenschaft und Gesellschaft: Wollen wir unsere IT-Sicherheit und damit unsere informationelle Selbstbestimmung zu einem Stück zugunsten unserer Sicherheit vor terroristischen Gefahren opfern? Denkbar wäre es auch, sich gegen die Staatstrojaner „aus der Ferne“ zu entscheiden. Das mag für die Sicherheitsbehörden unbequemer sein. Die Ausmaße einer Software wie „Pegasus“, deren vollständiger Schrecken erst nach und nach ans Licht kommt, sollten aber zumindest Anlass für

Diskussionen darüber geben, welche staatliche Handlung in diesem Fall das größere Sicherheitsrisiko darstellt.

Zitiervorschlag: Theresa Bosl, Ein Sieg für die Sicherheit – aber welche? Der Beschluss des BVerfG zur Nutzung von IT-Sicherheitslücken beim Einsatz von Staatstrojanern, JuWissBlog Nr. 80/2021 v. 5.8.2021, https://www.juwiss.de/80-2021/